UNITED STATES PATENT AND TRADEMARK OFFICE

Aw

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,293	07/06/2001	Young-Il Kim	P56339	7669

7590 06/16/2005

Robert E. Bushnell
Suite 300
1522 K Street N.W.
Washington, DC 20005-1202

EXAMINER	
ALOMARI, FIRAS B	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/899,293	**Applicant(s)** KIM, YOUNG-IL
	Examiner Firas Alomari	**Art Unit** 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/21/2001*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DTAILED ACTION

Response to Amendment

1. Applicant's arguments, see amendment, filed 03/09/2005, with respect to the rejection(s) of claim(s) 1-3 under Holloway et al. US (5,805,801) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Sofer et al. US (5,489,896).

2. Claims 4-21 have been added.

Claim Objections

1. Claims 16 and 18 are objected to under 37 CFR 1.121 as being in improper form because the proper status identifier (original) is incorrect. Appropriate correction is required.

2. Claim 18 is objected to because the claim is depending on claim 19. the examiner will interpret the claim to be dependent from claim 17.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-3 are rejected under 35 U.S.C. 102(b) as being anticipated by Holloway et al. US (5,805,801) in view of Sofer et al. US (5,489,896).

As per claims 1 and 19: Holloway discloses A MAC (media access control) address-based communication restricting method (Col 3, lines 15-16) comprising the steps of: Receiving packet data upon request of communication through at least one port of a plurality of ports of an Ethernet switch (Col16, lines 27-30);
Holloway teaches obtaining the destination MAC addresses through the discovery phase (item 145 of FIGF 10 and item 131 of FIG 11) but Holloway doesn't explicitly teach Reading a MAC destination address and a MAC source address included in the received packet data. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches the using of a MAC address stripper to extract the source and destination MAC addresses from a packet (Col 4, lines 13-22). therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to include a MAC stripper to extract the MAC destination and source addresses from the received packets. One would be motivated to do so in order to provide the

system with ability to determine where did the packet come form and where the packet is headed to and if it's headed to a protected destination.

Detecting In an address table, access vectors corresponding to the MAC destination and source address (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9 / Holloway teaches using combination of data structures AAL (access authorization List) and ICD (interconnected device list) the ICD will contain information on connected MAC addresses to the specific Managed hub while the AAL will contain the security access control information for each device. The combination of those two will perform the same function as the address table)

Denying access if the access vectors of the MAC destination and source addresses are not matched (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

As per claims 2 and 20: Holloway teaches the system further comprising steps of:

Configuring an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address; (Col 7, Lines 7-13 and FIG 7; Holloway method teaches the AAL table and Breach list table with no IP address but he also teaches in Col 17 lines 15-17 that the list can be extended to contain the IP address)

Determining whether the received MAC source address is stored in said address table (item 132 of FIG 11 and Col 11 lines 14-16); configuring an address entry for said received MAC source address when it is determined that said MAC source address is not stored in said address table and identifying said received MAC source address as a new MAC source address (item 135 of FIG 11, Col 11 lines 21-29, item 137 of FIG 11 and Col 11 lines 31-34);

Determining whether said new MAC source address is stored in said anti-hacker table (item 220 of FIG 12 and Col 11, lines 62-64); and

Storing the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-23).

Asp per claims 3,18 and 21: Holloway teaches the system further comprising:

Adding a port number, corresponding to the port through which said packet data was received, to a storage area corresponding to said new MAC source address in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-20);

Modifying an access vector included in said configured address entry for said new MAC source address, to set security (item 320 of FIG 13 and Col 13 lines 34-36 / setting the filter in Holloway system perform the task of setting security by defining which MAC addresses are allowed or denied access to the destination MAC addresses); and

Storing the configured address entry including the modified access for said new Mac source address in said address table (items 320,322 of FIG 13 and lines 34-41 / setting up the filter and checking if the filter has been applied, implies that the filter containing the MAC address is stored on the device memory).

Regarding claim 4: Holloway discloses a packet switch restricting MAC (media access control) address-based communication, comprising:

A host providing overall control to the packet switch and executing commands input to the packet switch; (Col 5, lines 13-19)

At least one MAC port performing MAC control operations and outputting transmit/receive command of a data packet; (Col 4, lines 67 through Col 5, lines line 1)

A transmission/reception controller receiving said transmit/receive command; (Col 5, lines 7-12)

A data exchange controlled by said transmission/reception controller, said data exchange establishes paths of data and control serials between the host, the MAC port and a packet memory;(Col 5, lines 2-12)

Said packet memory storing received data packets, said packet memory including a port table and an address table; (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9)

said port table storing information about a current status of the packet switch, port attributes and enable/disable, and packet reception completion of each MAC port; (Col 11, lines 44-50) and said address table storing registered MAC addresses, destination access vectors corresponding to destination MAC addresses of said registered MAC addresses. (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9 / Holloway teaches using combination of data structures AAL (access authorization List) and ICD (interconnected device list) the ICD will contain information on connected MAC addresses to the specific Managed hub while the AAL will contain the security access control information for each device) but he doesn't disclose reading the source MAC address included in the received data packet, and detecting the source access vector corresponding to the source MAC address and denying the requested communication if the source access vector and the destination access vector do not match. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches reading the source and destination MAC addresses included in the received data packet, and detecting the destination access vector corresponding to the source MAC address and denying the requested communication if the destination access vector and the source access vector do not match(Col 4, lines 14-31). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to read the source MAC address as well as the destination MAC address before allowing or denying communication. One would be motivated to do so in order to provide the system with more flexibility by allowing the system to set up rules based not just on the destination of the packets but on the source the packet originated from as well consequently enabling the system to restrict communication that are known to be from an offending source addresses.

Regarding claim 5: The packet switch as set forth in claim 4, said packet memory including further a packet descriptor storing information about each packet stored in the packet memory. (Col 5, lines 3-12)

Regarding claim 6: The packet switch as set forth in claim 5, wherein said packet information comprises packet connection information. (Col 5, lines 21-49)

Regarding claim 7: The packet switch as set forth in claim 4, further comprising a search memory storing information by which a MAC port, corresponding to the destination MAC address of a received data packet, is determined for data packet output. (Col 8, lines 2-12)

Regarding claim 8: the packet switch as set forth in claim 7, wherein said transmission/reception controller temporarily stores received data packets, accesses said search memory, checks whether the destination MAC address in a header of the received data packet has been registered, locates where the registered destination MAC address is stored in the address table, and determines a MAC port through which the received data packet is to be output. (Col 8, lines 2-12 and Col 11, lines 55-61)

Regarding claim 9: The packet switch as set forth in claim 4, wherein said host includes an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address. (Col 7, Lines 7-13 and FIG 7; Holloway method teaches the AAL table and Breach list table with no IP address but he also teaches in Col 17 lines 15-17 that the list can be extended to contain the IP address)

Regarding claim 10: Holloway discloses the packet switch as set forth in claim 4, wherein said transmission/reception controller receives a data packet upon request of communication through the MAC port reads the destination MAC address and detects the destination access vector corresponding to the destination MAC address and denies the requested communication based on the destination access vector but he doesn't disclose reading the source MAC address included in the received data packet, and detecting the destination access vector corresponding to the source MAC address and denying the requested communication if the destination access vector and the source access vector do not match. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches reading the source and destination MAC addresses included in the received data packet, and detecting the destination access vector corresponding to the source MAC address and denying the requested communication if the destination access vector and the source access vector do not match(Col 4, lines 14-31). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to read the source MAC address as well as the destination MAC address before allowing or denying communication. One would be motivated to do so in order to provide the system with more flexibility by allowing the system to set up rules based not just on the destination of the packets but on the source the packet originated from as well consequently enabling the system to restrict communication that are known to be from an offending source addresses.

Regarding claim 11: (new) The packet switch as set forth in claim 10, wherein said transmission/reception controller determines whether the received source MAC address is stored in said address table (item 132 of FIG 11 and Col 11 lines 14-16), configures an address entry for said received source MAC address when it is determined that said source MAC address is not stored in said address table and identities said received source MAC address as a new source MAC address. (item 135 of FIG 11, Col 11 lines 21-29, item 137 of FIG 11 and Col 11 lines 31-34);

Regarding claim 12: (new) The packet switch as set forth in claim 11, wherein said transmission/reception controller determines whether said new source MAC address is stored in said anti-hacker table (item 220 of FIG 12 and Col 11, lines 62-64), and stores the configured address entry for said received source MAC address in said address table when it is determined that said new source MAC address is not stored in said anti-hacker table. (item 265 of FIG 12 and Col 12 lines 17-23).

Regarding claim 13: (new) The packet switch as set forth in claim 11, wherein said transmission/reception controller adds a port number, corresponding to the port through which said packet data was received, to a storage area corresponding to said new MAC source address in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-20);
Modifying an access vector included in said configured address entry for said new MAC source address, to set security (item 320 of FIG 13 and Col 13 lines 34-36 / setting the filter in Holloway system perform the task of setting security by defining which MAC addresses are allowed or denied access to the destination MAC addresses); and
Storing the configured address entry including the modified access for said new Mac source address in said address table (items 320,322 of FIG 13 and lines 34-41 / setting up the filter and checking if the filter has been applied, implies that the filter containing the MAC address is stored on the device memory).

Regarding claim 14: Holloway discloses a method of restricting MAC (media access control) address-based communication through packet switch, said method comprising steps of:
storing destination MAC addresses in an address table; (Col 3, line 7-9) storing destination access vectors in said address table, said destination access vectors respectively corresponding to said destination MAC addresses; (Col 9, lines 49-51 and

Col 11, lines 44-50) comparing, upon receipt of a data packet, one of said destination access vectors corresponding to a destination MAC address received in said header of said data packet; (Col 8, lines 2-12) and preventing said MAC address-based communication when the compared source access vector does not match the destination access vector. (Col 3, Lines 9-11) but he doesn't disclose using the source MAC address in allowing or preventing communication based on the source address access vector. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches reading the source and destination MAC addresses included in the received data packet, and detecting the destination access vector corresponding to the source MAC address and denying the requested communication if the destination access vector and the source access vector do not match(Col 4, lines 14-31). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to read the source MAC address as well as the destination MAC address before allowing or denying communication. One would be motivated to do so in order to provide the system with more flexibility by allowing the system to set up rules based not just on the destination of the packets but on the source the packet originated from as well consequently enabling the system to restrict communication that are known to be from an offending source addresses.

Regarding claim 15: Holloway discloses the method as set forth in claim 14, said comparing step comprising the steps of:

Determining whether the received MAC source address is stored in said address table (item 132 of FIG 11 and Col 11 lines 14-16); configuring an address entry for said received MAC source address when it is determined that said MAC source address is not stored in said address table and identifying said received MAC source address as a new MAC source address (item 135 of FIG 11, Col 11 lines 21-29, item 137 of FIG 11 and Col 11 lines 31-34);

Determining whether said new MAC source address is stored in said a address table (item 220 of FIG 12 and Col 11, lines 62-64); when it is determined that said source MAC address and said destination MAC address are stored in said address table, reading the source access vectors corresponding to said source MAC address and the destination access vectors corresponding to a destination MAC address from said address table. (Col 11, lines 46-50)

Regarding claim 16: Holloway discloses the method as set forth in claim 15, further comprising a step of:

Configuring an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address; (Col 7, Lines 7-13 and FIG 7; Holloway method teaches the AAL table and Breach list table with no IP address but he also teaches in Col 17 lines 15-17 that the list can be extended to contain the IP address)

Regarding claim 17: Holloway discloses the method as set forth in claim 16, further comprising steps of:

Determining whether the received MAC source address is stored in said address table (item 132 of FIG 11 and Col 11 lines 14-16); configuring an address entry for said received MAC source address when it is determined that said MAC source address is not stored in said address table and identifying said received MAC source address as a new MAC source address (item 135 of FIG 11, Col 11 lines 21-29, item 137 of FIG 11 and Col 11 lines 31-34);

Determining whether said new MAC source address is stored in said anti-hacker table (item 220 of FIG 12 and Col 11, lines 62-64); and

Storing the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-23).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

6/10/05

FA